

# CRS Report for Congress

Received through the CRS Web

## Protection of Security-Related Information

**September 27, 2006**

Gina Marie Stevens and Todd B. Tatelman  
Legislative Attorneys  
American Law Division

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>27 SEP 2006</b>		2. REPORT TYPE <b>N/A</b>		3. DATES COVERED <b>-</b>	
4. TITLE AND SUBTITLE <b>Protection of Security-Related Information</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Congressional Research Service The Library of Congress 101 Independence Ave. SE Washington, DC 20540-7500</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release, distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>SAR</b>	18. NUMBER OF PAGES <b>29</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

# Protection of Security-Related Information

## Summary

The terrorist attacks of September 11 prompted a reevaluation of how to balance public access to information with the need for safety and security. The accumulation of confidential business information from owners and operators of the nation's critical infrastructures, 85% of which is reportedly owned by the private sector, continues to be an important component of homeland security efforts. Critical infrastructure sectors have been defined to include information technology; telecommunications; chemicals; transportation systems; including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; postal and shipping; agriculture and food; public health and healthcare; drinking water and water treatment systems; energy, including oil and gas and electric power; banking and finance; the defense industrial base; and national monuments and icons. The Freedom of Information Act of 1974 (FOIA) along with other statutes and regulations provide legal authorities for the protection of various types of security-related information. Nevertheless, some owners and operators are hesitant to voluntarily share security-related information with the government because of the possible disclosure of this information to the public. To prohibit public disclosure of security-related information under the Freedom of Information Act and other laws, Congress has drafted and passed legislation designed to remove legal obstacles to information sharing. The Aviation and Transportation Security Act of 2001 (ATSA); the Critical Infrastructure Information Act of 2002 in section 214 of the Homeland Security Act; the Maritime Transportation Security Act of 2002 (MTSA); and the Safe Drinking Water Act (SDWA), as amended by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, each exempt certain types of security-related information from disclosure under the Freedom of Information Act. These statutes are examples of what are referred to as FOIA exemption 3 statutes; separate federal statutes prohibiting the disclosure of a certain type of information and authorizing its withholding under FOIA subsection (b)(3).

This report describes the current state of the law with regard to the protection of security-related information.

## Contents

Introduction .....	1
The Freedom of Information Act (FOIA) .....	1
Exemption 4 — Commercial or Financial Information .....	4
Exemption 3 — Information Protected By Other Statutes .....	6
The Maritime Transportation Security Act of 2002 (MTSA) ....	9
The Aviation and Transportation Security Act 2001 (ATSA) ...	10
The Safe Drinking Water Act (SDWA) .....	10
Critical Infrastructure Information Act of 2002 (CIIA) .....	11
Definitions .....	11
Protected Critical Infrastructure Information (PCII) .....	12
Freedom of Information Act .....	13
Ex Parte Communications in Agency Proceedings .....	13
Prohibition on Use of PCII in Civil Actions .....	14
Prohibited and Protected Disclosures .....	14
Access under State and Local Laws .....	15
Waiver of Privileges .....	15
Federal Advisory Committee Act .....	15
Independently Obtained Information .....	16
Voluntary Submissions to the Government .....	17
Safeguards for PCII .....	17
Criminal Penalties .....	17
Other Provisions .....	18
Final Regulations .....	18
Air Transportation Security Act of 1974 .....	19
Sensitive Security Information (SSI) .....	19
Further Statutory Expansion of SSI Authority .....	20
Judicial Review of SSI Classification .....	23

# Protection of Security-Related Information

## Introduction

The terrorist attacks of September 11 prompted a limiting of public access to government information developed, obtained, or compiled for homeland security purposes. The accumulation of confidential business information from owners and operators of the nation's critical infrastructures, 85% of which is reportedly owned by the private sector, continues to be a critical component of homeland security efforts. Concerns that competitors, terrorists, and other "bad actors" might gain access to security-related information under the Freedom of Information Act (FOIA) prompted new confidentiality protections to promote information sharing between the private sector and the federal government and to prevent disclosure of certain types of security-related information under FOIA. The Aviation and Transportation Security Act of 2001 (ATSA); the Critical Infrastructure Information Act of 2002 in section 214 of the Homeland Security Act of 2002; the Maritime Transportation Security Act of 2002 (MTSA); and the Safe Drinking Water Act (SDWA), as amended by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, exempt certain types of security-related information from disclosure under the Freedom of Information Act. These statutes are examples of what are referred to as FOIA exemption 3 statutes; separate federal statutes prohibiting the disclosure of a certain type of information and authorizing its withholding under FOIA subsection (b)(3).

This report describes the current state of the law with regard to the protection of security-related information. The protection of security-related information has developed from a series of laws, regulations, and executive orders. This report does not apply to the maintenance, safeguarding, or disclosure of classified national security information.<sup>1</sup>

## The Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA) applies to records held by agencies of the executive branch of the federal government and regulates the disclosure of government information.<sup>2</sup> The FOIA requires agencies to publish in the *Federal Register* certain records, and to make other records available for public inspection

---

<sup>1</sup> For information on national security information, see CRS Report RL33502, *Protection of National Security Information*, by Jennifer K. Elsea; see also, Christina E. Wells, *National Security Information and the Freedom of Information Act*, 56 ADMIN. L. REV. 1195 (2004).

<sup>2</sup> 5 U.S.C. § 552 *et seq.*

and copying.<sup>3</sup> With the exception of three special categories of law enforcement-related records that are entirely excluded from the coverage of the FOIA and records already made available for publication or inspection, all other federal agency records may be requested under the FOIA.<sup>4</sup> That records are potentially

---

<sup>3</sup> 5 U.S.C. § 552(a)(1)-(2) provides:

- (a) Each agency shall make available to the public information as follows:
  - (1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public —
    - (A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;
    - (B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;
    - (C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;
    - (D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and
    - (E) each amendment, revision, or repeal of the foregoing. ....
  - (2) Each agency, in accordance with published rules, shall make available for public inspection and copying —
    - (A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;
    - (B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register;
    - (C) administrative staff manuals and instructions to staff that affect a member of the public;
    - (D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and
    - (E) a general index of the records referred to under subparagraph (D); unless the materials are promptly published and copies offered for sale.

<sup>4</sup> 5 U.S.C. § 552(a)(3) and (E) provides:

- (3)(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which
  - (i) reasonably describes such records and
  - (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.
- (E) An agency, or part of an agency, that is an element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a (4))) shall not make any record available under this paragraph to —

(continued...)

subject to FOIA requests does not mean they necessarily will be disclosed. Nine categories of information may be exempted from mandatory disclosure.<sup>5</sup> The exemptions permit, rather than require, the withholding of the requested information. Records that are not exempt under one or more of the Act's nine exemptions must be disclosed. If a record contains some exempt material, any reasonably segregable portion of the record must be provided to any person requesting such record after

---

<sup>4</sup> (...continued)

- (i) any government entity, other than a State, territory, commonwealth, or district of the United States, or any subdivision thereof; or
- (ii) a representative of a government entity described in clause (i).

<sup>5</sup> 5 U.S.C. § 552(b) provides:

(b) This section does not apply to matters that are —

- (1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and
- (B) are in fact properly classified pursuant to such Executive order;
- (2) related solely to the internal personnel rules and practices of an agency;
- (3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute
  - (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or
  - (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information
  - (A) could reasonably be expected to interfere with enforcement proceedings,
  - (B) would deprive a person of a right to a fair trial or an impartial adjudication,
  - (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,
  - (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,
  - (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or
  - (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (9) geological and geophysical information and data, including maps, concerning wells.

deletion of the portions which are exempt. Disputes over access to requested records may be reviewed in federal court to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld. The court shall determine the matter de novo, and may examine the contents of such agency records in camera. The burden is on the agency to sustain its action.<sup>6</sup>

On December 14, 2005, the President issued Executive Order 13392, entitled “Improving Agency Disclosure of Information,” and which contains several statements of FOIA policy and specific planning and reporting requirements for federal agencies. Executive Order 13392 directs federal agencies to improve their FOIA operations and designates a Chief FOIA Officer for each agency’s administration of the FOIA.<sup>7</sup>

#### **Exemption 4 — Commercial or Financial Information.**

One possible means of shielding security-related information is exemption 4. Exemption 4 of FOIA exempts from disclosure “trade secrets and commercial or financial information obtained from a person and privileged or confidential.”<sup>8</sup> Most exemption 4 cases have involved a dispute over whether the requested information was “confidential.”<sup>9</sup>

In 1974, the D.C. Circuit in *National Parks and Conservation Association v. Morton*,<sup>10</sup> enunciated a two-part confidentiality test for commercial information: “if disclosure of the information is likely to either impair the government’s ability to obtain necessary information in the future; or to cause substantial harm to the competitive position of the person from whom the information was obtained,” the commercial information will be treated as confidential.<sup>11</sup> In 1992, in *Critical Mass Energy Project v. NRC*,<sup>12</sup> the D.C. Circuit limited the scope and application of

---

<sup>6</sup> 5 U.S.C. § 552(4)(b) (2000).

<sup>7</sup> E.O. No. 13392.

<sup>8</sup> 5 U.S.C. § 552(b)(4).

<sup>9</sup> Federal agencies are required to establish procedures to notify submitters of confidential commercial information whenever an agency “determines that it may be required to disclose” such information under the FOIA. The submitter is provided an opportunity to submit objections to the proposed disclosure. If the agency decides to release the information over the objections of the submitter, the submitter may seek judicial review of the propriety of the release, and the courts will entertain a “reverse FOIA” suit to consider the confidentiality rights of the submitter. E.O. 12600, 3 C.F.R. 235 (1988), *reprinted in* 5 U.S.C. § 552 note.

<sup>10</sup> 498 F.2d 765 (D.C. Cir. 1974).

<sup>11</sup> *Id.* at 770.

<sup>12</sup> 975 F.2d 871, 879-80 (D.C. Cir. 1992) (*en banc*) (“*Critical Mass II*”), *cert. denied*, 113 S. Ct. 1579 (1993) (The plaintiff was seeking reports which a utility industry group prepared and gave voluntarily to the NRC. The agency did, however, have the authority to compel submission. Applying the customary treatment test to the utility industry group reports voluntarily submitted to the government, the D.C. Circuit agreed with the district court’s

(continued...)



*National Parks* to cases in which a FOIA request is made for commercial or financial information which is *required* to be furnished to the Government.<sup>13</sup> The court established a new test of confidentiality for information submitted voluntarily, under which information is exempt from disclosure if the submitter can show that it does not customarily release the information to the public.<sup>14</sup> The burden of establishing the submitter's custom remains with the agency seeking to withhold the record.<sup>15</sup>

A number of lower federal courts have applied the *Critical Mass* distinction between voluntary and required submissions.<sup>16</sup> Nonetheless, *Critical Mass* has not been widely adopted by the other circuits.<sup>17</sup>

Whether submission of a vulnerability assessment or a site security plan is voluntary or required will determine the level of protection afforded the information under exemption 4. Because an absolute prohibition on the disclosure of commercial or financial information does not exist under exemption 4,<sup>18</sup> separate confidentiality

---

<sup>12</sup> (...continued)

conclusion that the reports were commercial; that they were provided to the agency on a voluntary basis; and that the submitter did not customarily release them to the public. Thus, the reports were found to be confidential and exempt from disclosure under exemption 4.)

<sup>13</sup> *Id.* at 880.

<sup>14</sup> *Id.* at 879.

<sup>15</sup> The Department of Justice has issued policy guidance on the distinction between information required and information voluntarily submitted under *Critical Mass*. See *FOIA Update*, Vol. XIV, No. 2, at 3-5 ("OIP Guidance: The Critical Mass Distinction Under Exemption 4").

<sup>16</sup> See, e.g., *Lykes v. Bros. S.S. v. Pena*, No. 92-2780, slip op. at 8-11 (D.D.C. Sept. 2, 1993) ("under *Critical Mass*, submissions that are required to realize the benefits of a voluntary program are to be considered mandatory"); *Lee v. FDIC*, 923 F. Supp. 451, 454 (S.D.N.Y. 1996) (when documents were "required to be submitted" in order to get government approval to merge two banks, court rejects agency's attempt to nonetheless characterize submission as "voluntary"); *AGS Computers, Inc. v. United States Dep't of Treasury*, No. 92-2714, slip op. at 10 (D.N.J. Sept. 16, 1993) (submitter's submission of documents to agency during a meeting was done voluntarily because there was no "controlling statute, regulation, or written order"); *Center for Auto Safety v. National Highway Traffic Safety Admin.*, 93 F. Supp.2d 1 (D.D.C. Feb. 28, 2000), remanded by *Center for Auto Safety v. National Highway Traffic Safety Admin.*, 244 F.3d 144 (D.C. Cir. Mar. 30, 2001) (information on airbag systems submitted in response to agency's request was a voluntary submission because agency lacked legal authority to enforce its request for information).

<sup>17</sup> The Tenth Circuit adopted the *Critical Mass* distinction between voluntary and involuntary submissions in *Utah v. U.S. Dep't of Interior*, 256 F.3d 967, 969 (10<sup>th</sup> Cir. 2001); see also U.S. Department of Justice, FREEDOM OF INFORMATION ACT GUIDE AND PRIVACY ACT OVERVIEW at 284-304 (discussing cases), available at [<http://www.justice.gov/o4foia/foi-act.htm>].

<sup>18</sup> Some representatives of potential confidential business information submitters have expressed concerns about the discretionary nature of exemption 4 because an agency may choose to withhold information but is not required to do so. See James W. Conrad, (continued...)

protections have been created for certain types of security-related information under other federal statutes. Often the security-related statutes discussed herein differentiate between “required” and “voluntary” submission. For example, the Maritime Transportation Security Act (MTSA) and the Safe Drinking Water Act (SDWA) require covered entities to submit information to the federal government. The Critical Infrastructure Information Act (CIIA) provides confidentiality protections for critical infrastructure information voluntarily submitted to DHS. The regulations for sensitive security information issued pursuant to the Aviation and Transportation Security Act (ATSA) designate 16 categories of sensitive security information, and include information submitted pursuant to a requirement and information voluntarily submitted. These statutes are examples of what are referred to as a FOIA exemption 3 statutes; that is, separate federal statutes prohibiting the disclosure of a certain type of information and authorizing its withholding under FOIA subsection (b)(3).

**Exemption 3 — Information Protected By Other Statutes.** FOIA subsection (b)(3), commonly referred to as exemption 3, permits agencies to withhold information under FOIA that is specifically prohibited from disclosure by other federal statutes with certain characteristics.<sup>19</sup>

Special circumstances warrant special decisions about confidential status, and Congress is free to define what must and what can be withheld by laws that integrate with this exemption, a sort of catch-all provision to the Freedom of Information Act. Congress recognized that some situations simply do not fit the general mold of FOIA releases of agency records to any requester. This third exemption establishes an open-ended set of documents which have previously been mandated to be confidential or for which Congress has made specific provision for confidentiality. It is Congress, not the agency, which makes the secrecy decision under this exemption.<sup>20</sup>

For a nondisclosure provision in a separate federal statute to qualify for exemption 3 status, the nondisclosure provision must meet one or two of the criteria: either the statute must require that matters be withheld from the public in such a manner as to leave no discretion on the issue, or establish particular criteria for withholding or refer to particular types of matters to be withheld.<sup>21</sup> If the statute meets the criteria of exemption 3 of FOIA and the information to be withheld falls

---

<sup>18</sup> (...continued)

*Protecting Private Security-Related Information From Disclosure By Government Agencies*, 57 ADMIN. L. REV. 715, 730-732 (2005).

<sup>19</sup> 5 U.S.C. § 552(b)(3) provides

Information may be withheld under an Exemption 3 statute when that statute either “(A) requires that matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.”

<sup>20</sup> James. T. O’Reilly, *FEDERAL INFORMATION DISCLOSURE* § 13.1 (3d. ed. 2000).

<sup>21</sup> 5 U.S.C. § 552(b)(3).

within the scope and coverage of that statute, the information is properly exempt from disclosure under exemption 3 of FOIA.

To withhold a document under exemption 3, the agency bears the burden of demonstrating that the statute either requires that the document or documents be withheld without agency discretion<sup>22</sup> or specifically authorizes the agency to use discretion to withhold that type of document.<sup>23</sup> The scope of the statute must be examined by a reviewing court to determine whether it qualifies as a withholding statute. Basic principles of statutory construction are to be used to determine exemption 3 status.<sup>24</sup> When resolving an ambiguity about the proper interpretation of a specific statute under exemption 3, the *Chevron*<sup>25</sup> rule of judicial deference applies to the agency's interpretation of the statute it administers.<sup>26</sup> Substantial weight is to be given to an agency's claim of exemption 3 status.

The first subpart of exemption 3 — subpart (A) — is often referred to as the “no discretionary release” category.<sup>27</sup> To satisfy this requirement, the statute's language to withhold must be absolute — for example, stating that the information “shall not be disclosed.” To withhold a document under subpart (A) of exemption (b)(3), the agency must show that the document is collected or generated under the agency's statutory authority, and that the statute contained a mandate that this type of information not be disclosed. For example, the Supreme Court found no discretion within the Census Act's prohibition against disclosure of census records.<sup>28</sup>

Subpart (B) of exemption (b)(3), commonly referred to as the “particular criteria” category, permits agency discretion on whether to withhold or disclose agency records.<sup>29</sup> Under subpart (B), an agency has the discretion to disclose if it so chooses but also has authority (explicit or implicit) to withhold. The statute must establish particular criteria for withholding or refer to particular types of matters to be withheld. To qualify under subpart (B), the statute must provide articulable criteria for the agency to use to determine whether to permit disclosure. The Supreme Court looks for “sufficiently definite standards” in a statute rather than “broad discretion.”<sup>30</sup> The degree to which Congress has specified the agency's discretion in the statute is important. A court must examine the underlying

<sup>22</sup> See *American Jewish Congress v. Kreps*, 574 F.2d 624 (D.C. Cir. 1978); see also *Lee Pharmaceuticals v. Kreps*, 577 F.2d 610 (9<sup>th</sup> Cir. 1978).

<sup>23</sup> See *American Jewish Congress v. Kreps*, 574 F.2d 624 (D.C. Cir. 1978).

<sup>24</sup> See CRS Report 97-589, *Statutory Interpretation: General Principles and Recent Trends*, by George Costello.

<sup>25</sup> *Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984).

<sup>26</sup> *Tax Analysts v. I.R.S.*, 117 F.3d 607, 612 (D.C. Cir. 1997).

<sup>27</sup> 5 U.S.C. A. § 552(b)(3)(A), “in such a manner as to leave no discretion on the issue.”

<sup>28</sup> *Baldridge v. Shapiro*, 455 U.S. 345 (1982); see also 13 U.S.C. § 214 (2000).

<sup>29</sup> 5 U.S.C. § 552(b)(3)(B) “establishes particular criteria for withholding or refers to particular types of matters to be withheld.”

<sup>30</sup> *Consumer Product Safety Commission v. GTE Sylvania, Inc.*, 447 U.S. 102 (1980).

congressional intent to exempt material from FOIA and analyze the amount of discretion left to the agency. The statute must be “the product of congressional appreciation of the dangers inherent in airing particular data and must incorporate a formula whereby the administrator may determine precisely whether the disclosure in any instance would pose the hazard that Congress foresaw.”<sup>31</sup>

Numerous statutes have been held by courts to qualify as exemption 3 statutes and agencies.<sup>32</sup> In addition, agencies often rely on statutes as a basis for exemption 3 withholding in the absence of a judicial determination that the statute qualifies as an exemption 3 withholding statute.<sup>33</sup> Congress has increasingly enacted exemption 3 statutes containing disclosure prohibitions that are specifically directed toward the Freedom of Information Act (FOIA).<sup>34</sup> The following are summaries of selected exemption 3 statutes applied by various agencies that may be relevant to the protection of security-related information and that contain legal authorities or

<sup>31</sup> *Sciba v. Board of Governor of Federal Reserve System*, 2005 WL 758260 (D.D.C. 2005), (quoting *Wisconsin Project on Nuclear Arms Control v. U.S. Dept. of Commerce*, 317 F.3d 275, 280 (D.C. Cir. 2003); *American Jewish Congress v. Kreps*, 574 F.2d 624, 628-29 (D.C. Cir. 1978); *Whalen v. U.S. Marine Corps*, 2005 WL 736536 (D.D.C. 2005)).

<sup>32</sup> See 13 U.S.C. §§ 8(b) and 9(a) (prohibits use of Census Act data for secondary purposes); Fed. R. Crim. P. 6(e), requires secrecy for grand jury matters; 50 U.S.C. § 403-3(1)(5) protects CIA intelligence sources and methods; 26 U.S.C. § 6103, controls income tax return information; 35 U.S.C. § 122, prohibits disclosure of patent applications; 50 U.S.C. § 402, exempts from disclosure the organization or function of the National Security Agency; 15 U.S.C. § 2055(b)(1) governs the disclosure of information submitted to the Consumer Product Safety Commission; 42 U.S.C. § 2000e-8(e) of the Civil Rights Act of 1964 prohibits the disclosure of information reported to the Equal Employment Opportunity Commission.

<sup>33</sup> Department of Justice, Agencies Rely on Wide Range of Exemption 3 Statutes, FOIA Post (2003), *available at*, [<http://www.usdoj.gov/oip/foiapost/2003foiapost41.htm>].

<sup>34</sup> See, e.g., P.L. 107-296, § 214(a)(1)(A), 116 Stat. 2135 (2002) (prohibiting FOIA disclosure of critical infrastructure information voluntarily submitted to federal government for homeland security purposes) (enacted Nov. 25, 2002); 39 U.S.C. § 3016(d) (barring FOIA disclosure of documentary material provided pursuant to subpoena issued under statutory provision pertaining to nonmailable matter) (enacted Dec. 12, 1999); 42 U.S.C. § 7401 note (prohibiting FOIA disclosure of information submitted to EPA detailing “worst-case scenarios” that might result from accidental or intentional releases of chemicals or fuels) (enacted Aug. 5, 1999); 16 U.S.C. § 5937 (prohibiting FOIA disclosure of information pertaining to National Park System resources such as endangered species) (enacted Nov. 13, 1998); 38 U.S.C. § 7451 (prohibiting FOIA disclosure of certain information collected by Department of Veterans Affairs in surveys of rates of compensation) (enacted Aug. 15, 1990); 42 U.S.C. § 7412 (prohibiting FOIA disclosure of certain information acquired under Clean Air Act, 42 U.S.C. § 7412, if such information would pose threat to national security) (enacted Aug. 5, 1999); 31 U.S.C. § 3729 (prohibiting FOIA disclosure of certain information furnished pursuant to False Claims Act, 31 U.S.C. § 3729) (enacted Oct. 27, 1986); 31 U.S.C. § 5319 (preventing FOIA disclosure of Currency Transaction Reports) (enacted Sept. 13, 1982); 15 U.S.C. § 57b-2(f) (prohibiting FOIA disclosure of information received by FTC for investigative purposes) (enacted May 28, 1980); 15 U.S.C. § 1314(g) (proscribing FOIA disclosure of certain records gathered in course of investigations under Antitrust Civil Process Act (enacted Sept. 30, 1976)).

requirements regarding non-disclosure of information developed or obtained in accordance with those Acts.

The Electronic Freedom of Information Act Amendments of 1996 require agencies to list the exemption 3 statutes upon which they rely in their annual FOIA reports, and include a description of whether a court has upheld the agency's decision to withhold information under such statute.<sup>35</sup> An examination of exemption 3 statutes applied by DHS components throughout FY2004 reveals that several non-disclosure provisions are relied on to withhold security-related information.<sup>36</sup> These exemption (b)(3) statutes include non-disclosure provisions for critical infrastructure information,<sup>37</sup> the prohibition on release of all information contained in maritime industry vulnerability assessments,<sup>38</sup> the prohibition on release of all information contained in maritime security plans,<sup>39</sup> and a provision governing the non-disclosure of transportation security activities.<sup>40</sup> The Environmental Protection Agency cites a provision of the Safe Drinking Water Act<sup>41</sup> as authority to withhold vulnerability assessments from community water systems under exemption 3.<sup>42</sup>

***The Maritime Transportation Security Act of 2002 (MTSA).***<sup>43</sup> An exemption 3 statute administered by the U.S. Coast Guard, The MTSA requires ports and facilities located within ports to perform vulnerability assessments and develop security plans. The MTSA requires “an owner or operator of a vessel or facility ... [to] prepare and submit to the Secretary a security plan for the vessel or facility.”<sup>44</sup> The reach of this requirement can be quite broad. For example, because ports are often the location of chemical facilities, such as petroleum refineries, some chemical facilities must comply with MTSA.<sup>45</sup> The MTSA provides that information developed under this statute *is not required* to be disclosed to the public.<sup>46</sup> Covered information includes “facility security plans, vessel security plans, and port

---

<sup>35</sup> P.L. 104-231, 5 U.S.C. § 552(e)(1)(B)(ii).

<sup>36</sup> Department of Homeland Security Privacy Office, 2005 Annual Freedom of Information Act Report to the Attorney General of the United States: October 1 - September 30, 2005, 8, *available at*, [[http://www.dhs.gov/interweb/assetlibrary/privacy\\_rpt\\_foia\\_2005.pdf](http://www.dhs.gov/interweb/assetlibrary/privacy_rpt_foia_2005.pdf)].

<sup>37</sup> 6 U.S.C. § 133.

<sup>38</sup> 46 U.S.C. § 1114(s).

<sup>39</sup> 46 U.S.C. § 70103.

<sup>40</sup> 49 U.S.C. § 114(s).

<sup>41</sup> 42 U.S.C. § 1433 (a)(3).

<sup>42</sup> Environmental Protection Agency, FY2004 Annual Freedom of Information Report, 5, *available at* [<http://www.epa.gov/foia/docs/2004report.pdf>].

<sup>43</sup> Homeland Security Act of 2002, P.L. 107-295.

<sup>44</sup> 46 U.S.C. § 70103(c)(1).

<sup>45</sup> See CRS Report RL33043, *Legislative Approaches to Chemical Facility Security*, by Dana A. Shea.

<sup>46</sup> 46 U.S.C. § 70103(d) (stating that “[n]otwithstanding any other provision of law, information developed under this chapter is not required to be disclosed to the public ...”).

vulnerability assessment; and ... other information related to security plans, procedures, or programs for vessels or facilities authorized under this chapter.”<sup>47</sup>

***The Aviation and Transportation Security Act 2001 (ATSA).*** The ATSA transferred to the Transportation Security Administration (TSA) responsibility for protection of certain information vital to transportation security.<sup>48</sup> ATSA provides that “notwithstanding section 552 of title 5 and the establishment of a Department of Homeland Security, the Secretary of Transportation shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring security under this title if the Secretary of Transportation decides disclosing the information would - (A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to transportation safety.”<sup>49</sup> The Secretary of Transportation issued regulations covering the disclosure of a category of information labeled sensitive security information (SSI).<sup>50</sup>

***The Safe Drinking Water Act (SDWA).*** The SDWA, as amended by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002,<sup>51</sup> among other things requires community water systems to perform vulnerability analyses of their facilities and includes protections for vulnerability assessments.<sup>52</sup> Community water systems are required to certify to EPA that they have conducted a vulnerability assessment, and to submit a copy of the assessment to EPA. The SDWA requires that “(2) each community water system ... [shall] certify to the Administrator that the system has conducted an assessment ... and shall submit to the Administrator a written copy of the assessment.”<sup>53</sup> The SDWA provides that “all information provided to the Administrator [of the EPA] under this subsection and all information derived therefrom shall be exempt from disclosure under section 552 of Title 5.”<sup>54</sup>

---

<sup>47</sup> *Id.*; see also *infra*, notes 99-106 and accompanying text.

<sup>48</sup> Aviation and Transportation Security Act, P.L. 107-71, §101(e)(3), 115 Stat. 597, 603 (2001) (codified at 49 U.S.C. § 40119 (2001)). The D.C. Circuit has held that this provision of the Federal Aviation Act relating to security data the disclosure of which would be detrimental to the safety of travelers shields that particular data from disclosure under the FOIA. *Pub. Citizen, Inc. v. FAA*, 988 F.2d 186, 194 (D.C. Cir. 1993).

<sup>49</sup> See CRS Report RL33512, *Transportation Security: Issues for the 109<sup>th</sup> Congress*, coordinated by David Randall Peterman.

<sup>50</sup> 49 C.F.R. Part 1520; see also *infra*, notes 93-98 and accompanying text.

<sup>51</sup> P.L. 107-188, 42 U.S.C. § 300i-2.

<sup>52</sup> See CRS Report RL31294, *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions*, by Mary Tiemann.

<sup>53</sup> 42 U.S.C. § 300i-2(a)(2).

<sup>54</sup> 42 U.S.C. § 300i-2(a)(3).

## Critical Infrastructure Information Act of 2002 (CIIA)

The “Critical Infrastructure Information Act of 2002,” (“CIIA”) is found in Subtitle B of Title II of the Homeland Security Act of 2002.<sup>55</sup> CIIA consists of a group of provisions that address the circumstances under which the Department of Homeland Security may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection program. The CIIA was enacted, in part, to respond to the need for the federal government and owners and operators of the nation’s critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public sectors in order to protect critical assets. CIIA establishes several limitations on the disclosure of critical infrastructure information voluntarily submitted to DHS.

### Definitions.

The CIIA includes 4 key definitions: critical infrastructure information; covered federal agency; voluntary; and express statement. Another key definition, critical infrastructure, is defined elsewhere in the Homeland Security Act.

The most important definition in CIIA is that of “critical infrastructure information” because the CIIA protections are triggered only for such information. Critical infrastructures are defined elsewhere in the Homeland Security Act as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.”<sup>56</sup> This definition is viewed as a broad catch-all provision likely to cover a wide array of activities.

*Critical infrastructure information* is defined as “information not customarily in the public domain and related to the security of critical infrastructure or protected systems —

- (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health and safety;
- (B) the ability of critical infrastructure or protected systems to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or,
- (C) any planned or past operational problem or solution regarding critical infrastructure ... including repair, recovery, reconstruction, insurance, or

---

<sup>55</sup> Homeland Security Act of 2002, P.L. 107-296, §§ 211-215 116 Stat. 2135 (2002).

<sup>56</sup> P.L. 107-56, § 1016(e), 42 U.S.C. 5195(e).

continuity to the extent it relates to such interference, compromise, or incapacitation.<sup>57</sup>

This definition covers a wide range of information and is further expanded by reference to the statutory definition of critical infrastructure from the USA PATRIOT Act.<sup>58</sup>

A covered federal agency is defined by the CIIA as the Department of Homeland Security.<sup>59</sup>

The term “voluntary” with respect to the submittal of critical infrastructure information to a covered federal agency means “the submittal thereof in the absence of such agency’s exercise of legal authority to compel access or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.”<sup>60</sup> In addition, the definition of voluntary includes a critical exclusion. A voluntary submission to DHS does not include filings that were also made with the Securities and Exchange Commission or Federal banking regulators, statements made pursuant to the sale of securities, or information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings. Consequently, information falling within the exclusion would not be protected from disclosure.

In order to obtain the protections of the CIIA, the submission must be accompanied by an express statement of expectation of protection from disclosure. In the case of written information or records, this means a written marking on the information or records similar to “This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.” In the case of oral information, CIIA requires the submission of a similar written statement within a reasonable time period following the oral communication.<sup>61</sup>

### **Protected Critical Infrastructure Information (PCII).**

Section 214 of the CIIA is entitled “Protection of Voluntarily Shared Critical Infrastructure Information.” The section establishes several protections for critical infrastructure information voluntarily submitted to the Department of Homeland Security for use regarding the security of critical infrastructures and protected systems and for other purposes when such information is accompanied by an express statement to the effect that the information is voluntarily submitted to the federal

---

<sup>57</sup> P.L. 107-296, § 212(3).

<sup>58</sup> See the “Issues and Concerns” section of CRS Report RL31547, *Critical Infrastructure Information Disclosure and Homeland Security* by John Moteff and Gina Marie Stevens.

<sup>59</sup> P.L. 107-296, 116 Stat. 2135, § 212(2); *See also id.* at § 214(c) (adding that the provision does not apply to “independently obtained information”).

<sup>60</sup> P.L. 107-296, § 212(7).

<sup>61</sup> *See id.* at § 214(a)(2)(A)-(B)



government in expectation of protection from disclosure. To encourage private and public sector entities and persons to voluntarily share their critical infrastructure information with the Department of Homeland Security, the CIIA includes several measures to ensure against disclosure of protected critical infrastructure information by DHS.

### ***Freedom of Information Act.***

Section 214(a)(1) of the CIIA, entitled “In General,” provides:

Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructures and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement....

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act).<sup>62</sup>

According to the Department of Justice, the agency responsible for administering the FOIA, section 214(a)(1) will operate as a new “Exemption 3 statute”<sup>63</sup> under FOIA.<sup>64</sup> Section 214(a)(1)(A) leaves no discretion and requires that critical infrastructure information voluntarily submitted to the DHS not be disclosed under FOIA.

### ***Ex Parte Communications in Agency Proceedings.***

Section 214(a)(1)(B) of the CIIA provides that PCII will not be subject to agency rules or judicial doctrine regarding ex-parte communications. The Administrative Procedure Act (APA) establishes the rules for agencies to adhere to with respect to ex parte communications in agency proceedings.<sup>65</sup> The APA defines an “ex parte communication” as an “oral or written communication not on the public record with respect to which reasonable prior notice to all parties is not given....”<sup>66</sup> Section 556(e) of the Administrative Procedure Act incorporates the principle that formal agency adjudications are to be decided solely on the basis of record evidence. It provides that “[t]he transcript of testimony and exhibits, together with all papers

---

<sup>62</sup> P.L. 107-296, 116 Stat. 2135, § 214(a)(1)(A) (codified at 6 U.S.C. § 133(a)(1)(A)).

<sup>63</sup> Under exemption 3 of the FOIA, information protected from disclosure under other statutes is also exempt from public disclosure provided that such statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or establishes particular criteria for withholding or refers to particular types of matters to be withheld. Unlike other FOIA exemptions, if the information requested under FOIA meets the withholding criteria of exemption 3, the information must be withheld. *See* 5 U.S.C. § 552(b)(3).

<sup>64</sup> Department of Justice, “Homeland Security Law Contains New Exemption 3 Statute,” FOIA Post (2003).

<sup>65</sup> 5 U.S.C. § 551 *et seq.*

<sup>66</sup> 5 U.S.C. § 551(14).

and requests filed in the proceeding, constitutes the exclusive record for decision.”<sup>67</sup> The reason for this “exclusiveness of record” principle is to provide fairness to the parties in order to ensure meaningful participation. Challenges to the “exclusiveness of record” occur when there are ex parte contacts — communications from an interested party to a decision making official that take place outside the hearing and off the record.

Section 557(d)(1) of the APA prohibits any “interested person outside the agency” from making, or knowingly causing, “any ex parte communication relevant to the merits of the proceeding” to any decision making official. Similar restraints are imposed on the agency decision makers.<sup>68</sup> When an improper ex parte contact occurs, the APA requires that it be placed on the public record; if it was an oral communication, a memorandum summarizing the contact must be filed.<sup>69</sup> Upon receipt of an ex parte communication knowingly made or knowingly caused to be made by a party in violation of the APA, the agency, administrative law judge, or other employee presiding at the hearing may require the party to show cause why his claim or interest in the proceeding should not be dismissed, denied, disregarded, or otherwise adversely affected on account of such violation.<sup>70</sup>

### ***Prohibition on Use of PCII in Civil Actions.***

Section 214(a)(1)(C) of the CIIA creates an evidentiary exclusion for PCII. Section 214(a)(1)(C) prohibits the direct use, without the written consent of the information submitter, of protected critical infrastructure information by such agency (DHS), any other federal, state, or local authority, or third party in any civil action arising under federal or state law if submitted in good faith. This evidentiary limitation does not apply to regulatory or enforcement actions by federal, state, or local governmental entities, nor to civil actions when the information is obtained independently of the DHS. Public interest groups are concerned that this provision is very broad, and potentially could shield owners and operators from liability under antitrust, tort, tax, civil rights, environmental, labor, consumer protection, and health and safety laws.

### ***Prohibited and Protected Disclosures.***

Section 214(a)(1)(D) of the CIIA prohibits use or disclosure of critical infrastructure information by U.S. officers or employees, without consent, for unauthorized purposes. This section authorizes the use or disclosure of such information by officers and employees in furtherance of the investigation or the prosecution of a criminal act; or for disclosure to Congress or the Government Accountability Office. The President’s signing statement accompanying the Homeland Security Act of 2002 expressly addressed this provision. It states that “The executive branch does not construe this provision to impose any independent

---

<sup>67</sup> *Id.* at § 556(e).

<sup>68</sup> 5 U.S.C. § 557(d)(1)(E).

<sup>69</sup> *Id.* at § 557(d)(1)(C).

<sup>70</sup> *Id.* at § 557(D).

or affirmative requirement to share such information with the Congress or the Comptroller General and shall construe it in any manner consistent with the constitutional authorities of the President to supervise the unitary executive branch and to withhold information the disclosure of which could impair foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties.”<sup>71</sup>

### ***Access under State and Local Laws.***

Section § 214(a)(1)(E) of the CIIA specifically mandates that the critical infrastructure information now exempt under the FOIA “shall not, if provided to a State or local government ... be made available pursuant to any State or local law requiring disclosure of information or records.” This statute thus explicitly provides for the “preemption” of state freedom of information laws by federal law.<sup>72</sup> It also prohibits state or local governments from disclosing protected critical infrastructure information provided to them by DHS without written consent of the entity submitting the information, and further prohibits its use for other than critical infrastructure protection, or the furtherance of a criminal investigation or prosecution.

### ***Waiver of Privileges.***

Section 214(a)(1)(F) of the CIIA guards against “waiver of any applicable privilege or protection provided under law, such as trade secret protection.” Other relevant evidentiary privileges may include the attorney-client privilege.<sup>73</sup>

### ***Federal Advisory Committee Act.***

Section 214(b) of the Act provides that no communication of critical infrastructure information to the Department of Homeland Security pursuant to the CIIA shall be considered an action subject to the requirements of the Federal Advisory Committee Act (FACA).<sup>74</sup> The FACA requires that meetings of federal advisory committees serving executive branch entities be open to the public.<sup>75</sup> The

---

<sup>71</sup> The White House, Statement by the President on H.R. 5005, the Homeland Security Act of 2002 (Nov. 25, 2002).

<sup>72</sup> See also *Freedom of Information Act Guide & Privacy Act Overview* (May 2002), at 563-64 (discussing operation of “preemption doctrine” in FOIA context).

<sup>73</sup> See Fed. R. Evid. 501.

<sup>74</sup> 5 U.S.C. App. 2.

<sup>75</sup> 5 U.S.C. App. 2, § 3(2) provides

An “advisory committee” means “any committee, board, commission, council, conference, panel, task force, or other similar group, or any subcommittee or other subgroup thereof (hereafter in this paragraph referred to as ‘committee’), which is - (A) established by statute or reorganization plan, or (B) established or utilized by the President, or (C) established or utilized by one or more agencies, in the interest of obtaining advice or recommendations for the President or one

(continued...)

FACA also specifies nine categories of information, similar to those in FOIA, that may be permissively relied upon to close advisory committee deliberations.

Prior to passage of the CIIA, meetings of Information Sharing and Analysis Organizations (ISAO) could potentially be subject to FACA's requirements.<sup>76</sup> However, the CIIA expressly authorizes ISAOs to voluntarily submit information to the DHS on behalf of itself or its members with the result being that such information will be protected in material respects under the Act from uses and disclosures unrelated to critical infrastructure protection.<sup>77</sup> For a discussion of information sharing and analysis centers formed by several sectors (e.g., banking and finance, telecommunications, electricity, water, etc.), see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John Moteff.

### **Independently Obtained Information.**

Section § 214(c) provides that a Federal entity may separately obtain critical infrastructure information submitted to the DHS for its critical infrastructure protection program through the use of independent legal authorities, and use such information in any action.<sup>78</sup> The CIIA does not limit the ability of governments, entities, or third parties to independently obtain critical infrastructure information or to use critical infrastructure information for limited purposes.

---

<sup>75</sup> (...continued)

or more agencies or officers of the Federal Government, except that such term excludes (i) any committee that is composed wholly of full-time, or permanent part-time, officers or employees of the Federal Government, and (ii) any committee that is created by the National Academy of Sciences or the National Academy of Public Administration.”

<sup>76</sup> P.L. 107-296, § 212(5) defines “Information Sharing and Analysis Organization” as

any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of — (A) gathering and analyzing critical infrastructure information ... (B) communicating or disclosing critical infrastructure information ... and (C) voluntarily disseminating critical infrastructure information....

<sup>77</sup> *Id.* at § 212(7)

<sup>78</sup> Subsection § 214(c) provides: “(c) INDEPENDENTLY OBTAINED INFORMATION- Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.”

## **Voluntary Submissions to the Government.**

Section 214(d) provides that the voluntary submittal to the government of information or records that are protected from disclosure shall not be construed to constitute compliance with any requirement to submit such information to a federal agency under any other law. Prior to the enactment of this new FOIA exemption 3 statute, critical infrastructure information submitted to the government would probably have fallen under exemption 4 (commercial or financial information) and its release under FOIA dependent on whether it was submitted voluntarily or pursuant to requirement. The Report of the House Select Committee on Homeland Security accompanying H.R. 5005 states that “The Select Committee intends that subtitle C only protect private, security-related information that is *voluntarily shared* with the government in order to assist in increasing homeland security. This subtitle does not protect information required under any health, safety, or environmental law” (emphasis added).<sup>79</sup>

## **Safeguards for PCII.**

Section 214(e) requires the Secretary of DHS to establish procedures for the receipt, care, and storage of critical infrastructure information not later than 90 days after enactment.<sup>80</sup> The Secretary of Homeland Security is to consult with the National Security Council and the Office of Science and Technology Policy to establish uniform procedures.

## **Criminal Penalties.**

Section 214(f) contains a provision that makes it a criminal offense for any federal employee to “knowingly ... disclose[] ... any critical infrastructure information [that is] protected from disclosure” under it, without proper legal authorization.

(f) PENALTIES- Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

---

<sup>79</sup> H. Rep. No. 107-609, Homeland Security Act of 2002, p. 116.

<sup>80</sup> The Homeland Security Act took effect 60 days after passage; the legislation was enacted on November 25, 2002. The Secretary was to establish those procedures no later than February 23, 2003.

This provision is similar to the criminal penalties imposed in the Privacy Act<sup>81</sup> and the Trade Secrets Act.<sup>82</sup>

### **Other Provisions.**

Section 214(g) of the CIIA authorizes the federal government to provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to critical infrastructure. In issuing a warning, the federal government must protect from disclosure the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning, or information that is proprietary, business sensitive, or otherwise not appropriately in the public domain.

Section 215 of CIIA expressly provides that a private right of action for enforcement of the Act is not created.

### **Final Regulations.**

The Department of Homeland Security recently promulgated the final rule for “Procedures for Handling Protected Critical Infrastructure Information.”<sup>83</sup> This final rule, which became effective upon publication in the Federal Register September 1, 2006, amends Homeland Security regulations establishing uniform procedures to implement the Critical Infrastructure Information Act of 2002. These procedures govern the receipt, validation, handling, storage, marking and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security. This rule applies to all federal agencies, all United States Government

---

<sup>81</sup> 5 U.S.C. § 552a (i)(1)(“ Criminal Penalties. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.”)

<sup>82</sup> 18 U.S.C. § 1905 (Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Office of Federal Housing Enterprise Oversight, or agent of the Department of Justice as defined in the Antitrust Civil Process Act (15 U.S.C. 1311-1314), publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.”).

<sup>83</sup> 71 Fed. Reg. 52,261 (Sept. 1, 2006), *available at* [<http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-7378.htm>].

contractors, and state, local and other governmental entities that handle, use, store, or have access to critical infrastructure information that enjoys protection under the Critical Infrastructure Information Act of 2002.

## Air Transportation Security Act of 1974

**Sensitive Security Information (SSI).** The law governing SSI originated with the Air Transportation Security Act of 1974 (1974 Act),<sup>84</sup> which delegated authority for transportation security to various agencies within the Department of Transportation (DOT). The 1974 Act specifically authorized the Federal Aviation Administration (FAA) to:

prohibit disclosure of any information obtained or developed in the conduct of research and development activities ... if in the opinion of the Administrator the disclosure of such information — (A) would constitute an unwarranted invasion of personal privacy...; (B) would reveal trade secrets or privileged or confidential commercial or financial information obtained from any person; or (C) would be detrimental to the safety of persons traveling in air transportation.<sup>85</sup>

The FAA implemented this authority by promulgating regulations, which, *inter alia*, established a category of information known as SSI. As late as 1997, the DOT's definition of SSI included "records and information ... obtained or developed during security activities or research and development activities."<sup>86</sup> Encompassed within this definition were airport and air carrier security programs, as well as specific details concerning aviation security measures. Consistent with this grant of authority, the FAA limited the applicability of the SSI regulation to airport operators, air carriers, and other air transportation related entities and personnel.

After the attacks of September 11, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), which, in addition to creating new security mandates, established the Transportation Security Administration (TSA) within DOT, and transferred the responsibility for aviation security to the newly created Under Secretary of Transportation for Security.<sup>87</sup> Among the legal authorities transferred to the Under Secretary was the protection of certain information vital to transportation security, or SSI.<sup>88</sup> In addition to transferring SSI classification authority to TSA, the ATSA eliminated the statute's specific reference to air transportation, thereby expanding the categories of information that can be classified

---

<sup>84</sup> Air Transportation Security Act of 1974, P.L. 93-366, § 316, 88 Stat. 409 (1974).

<sup>85</sup> *Id.*

<sup>86</sup> 14 C.F.R. § 191.1 (1997).

<sup>87</sup> The Under Secretary for Transportation Security is also known as the Administrator of TSA.

<sup>88</sup> Aviation and Transportation Security Act, P.L. 107-71, §101(e)(3), 115 Stat. 597, 603 (2001) (codified at 49 U.S.C. § 40119 (2001)).

as SSI.<sup>89</sup> This statutory change appears to permit TSA to protect SSI with respect to virtually all forms of interstate travel, including airplanes, buses, trains, and boats.

Initially, TSA and DOT issued regulations that in large part simply transferred the aviation security regulations, including SSI classification authority, from the FAA to TSA.<sup>90</sup> With respect to SSI, the regulations first noted the expansion of authority to all modes of transportation.<sup>91</sup> Given this expansion, the agency determined that while the Under Secretary was given the ultimate responsibility for carrying out the statute, it was most efficient for the other DOT operating administrators (i.e., railway, highway, transit, and pipeline) to have day-to-day responsibility over SSI in their own modes of transportation.<sup>92</sup>

**Further Statutory Expansion of SSI Authority.** In 2002, Congress enacted two statutes, the Maritime Transportation Security Act (MTSA)<sup>93</sup> and the Homeland Security Act of 2002,<sup>94</sup> both of which have had a significant impact on the scope and applicability of SSI. The first statute, MTSA, requires, *inter alia*, the Secretary of Homeland Security<sup>95</sup> to prepare a National Maritime Transportation Security Plan.<sup>96</sup> As a part of the national plan, the Secretary is required to identify specific vulnerable areas around the country for which Area Security Plans will be developed.<sup>97</sup> In addition, the MTSA requires owners and operators of vessels and facilities to develop and submit to the Secretary security plans that will be implemented to deter security incidents to the maximum extent practicable.<sup>98</sup> Finally, the MTSA provides that the information developed under this statute is not to be disclosed to the general public.<sup>99</sup> The non-disclosure provision encompasses all

<sup>89</sup> See Aviation and Transportation Security Act, P.L. 107-71, §101(e)(3), 115 Stat. 597, 603 (2001).

<sup>90</sup> See generally, 67 Fed. Reg. 8340 (Feb. 22, 2002).

<sup>91</sup> See *id.* at 8342.

<sup>92</sup> See *id.*

<sup>93</sup> See Maritime Transportation Security Act of 2002, P.L. 107-295, § 102(a) 116 Stat. 2068 (2002) [hereinafter MTSA].

<sup>94</sup> See Homeland Security Act of 2002, P.L. 107-296, § 1704(a) 116 Stat. 2135, 2314 (2002).

<sup>95</sup> The statute specifically references the “the Secretary of the department in which the Coast Guard is operating.” See MTSA, *supra* note 10 at § 102(a) (codified at 46 U.S.C. § 70110(5)). Currently, the Coast Guard is operating under the Department of Homeland Security. See Homeland Security Act, *supra* note 11 at § 1704(a) (amending the Coast Guard’s authorizing statute, 14 U.S.C. § 1, by replacing “Department of Transportation” with “Department of Homeland Security”).

<sup>96</sup> See MTSA, *supra* note 10 at § 102(a) (codified as amended at 46 U.S.C. § 70103(a) (2002)).

<sup>97</sup> See *id.* (codified as amended at 46 U.S.C. § 70103(b) (2002)).

<sup>98</sup> See *id.* (codified as amended at 46 U.S.C. § 70103(c) (2002)).

<sup>99</sup> *Id.* (codified as amended at 46 U.S.C. § 70103(d)) (stating that “[n]otwithstanding any (continued...)”).



“facility security plans, vessel security plans, and port vulnerability assessments; and ... other information related to security plans, procedures, or programs for vessels or facilities authorized under this chapter.”<sup>100</sup> The non-disclosure language, however, makes no reference to the information being classified as SSI, nor does it specifically refer in any way to the TSA and its statutory authority to regulate transportation security information.

In addition to MTSA, Congress also passed the Homeland Security Act of 2002, which, *inter alia*, transferred TSA, along with its SSI classification authority, to the newly created Department of Homeland Security (DHS).<sup>101</sup> The transfer of authority, however, required that TSA “shall be maintained as a distinct entity within the Department under the Under Secretary for Border Transportation.”<sup>102</sup> This distinct entity requirement was effective for the first two years of DHS’s existence and expired on November 25, 2004.<sup>103</sup> It should be noted that TSA was not the only agency that was transferred to DHS as a distinct entity. Other such agencies include the Coast Guard<sup>104</sup> and the United States Secret Service, whose status as distinct entities, however, unlike TSA’s, do not contain sunset provisions.<sup>105</sup>

The Homeland Security Act of 2002 also re-codified and further amended TSA’s authority to:

prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71) or under chapter 449 of this title if the Under Secretary decides that disclosing the information would — (A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to the security of transportation.<sup>106</sup>

In addition to the amendment to the definition of SSI, the Homeland Security Act of 2002 specifically prohibits the Under Secretary from transferring its SSI classification authority to “another department, agency, or instrumentality of the United States,” unless otherwise authorized by law.<sup>107</sup> Moreover, the Homeland Security Act of 2002 amended the existing DOT authority with respect to SSI such

---

<sup>99</sup> (...continued)

other provision of law, information developed under this chapter is not required to be disclosed to the public ...”)

<sup>100</sup> *Id.*

<sup>101</sup> *See generally*, Homeland Security Act, *supra* note 94.

<sup>102</sup> *See id.* at § 424(a).

<sup>103</sup> *Id.* at § 424(b) (stating that “subsection (a) shall expire 2 years after the date of enactment of this Act”).

<sup>104</sup> *See id.* at § 888.

<sup>105</sup> *See id.* at § 821.

<sup>106</sup> *See id.* at § 1601(b) (codified as amended at 49 U.S.C. § 114(s) (2002)).

<sup>107</sup> *See id.* (codified at 49 U.S.C. § 114(s)(3) (2002)).

that it would be virtually identical to the TSA authority.<sup>108</sup> The only difference between the two statutes is contained in subpart (C), which provides DOT with authority to prohibit disclosure of information that would be “detrimental to transportation safety.”<sup>109</sup> By removing any reference to persons or passengers, Congress again significantly broadened the scope of the SSI authority. As a result, it appears that the authority to designate information as SSI now encompasses all transportation related activities including air and maritime cargo, trucking and freight transport, as well as pipelines.

On May 18, 2004, TSA, functioning as distinct entity within DHS, and DOT jointly promulgated revised SSI regulations in response to their newly expanded statutory authority.<sup>110</sup> These revised regulations adopt the Homeland Security Act language as the definition of SSI. In addition, the new regulations incorporate former SSI provisions, including the sixteen categories of information and records that constitute SSI. Included among these categories are: security programs and contingency plans;<sup>111</sup> security directives;<sup>112</sup> security measures;<sup>113</sup> security screening information;<sup>114</sup> and a general category consisting of “other information.”<sup>115</sup> With

---

<sup>108</sup> See *id.* (codified as amended at 49 U.S.C. § 40119 (2002)).

<sup>109</sup> *Id.*

<sup>110</sup> See 69 Fed. Reg. 28066, 28069 (May 18, 2004).

<sup>111</sup> This section includes

any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including: — (i) Any aircraft operator or airport operator security program or security contingency plan under this chapter; ... (iii) Any national or area security plan prepared under 46 U.S.C. 70103;....

See 49 CFR § 1520.5(b)(1) (2004).

<sup>112</sup> Defined as “any Security Directive or order: (i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority; (ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or (iii) Any comments, instructions, and implementing guidance pertaining thereto. See 49 CFR § 1520.5(b)(2) (2004).

<sup>113</sup> Defined as including

specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including — (i) Security measures or protocols recommended by the Federal government; (ii) Information concerning the deployments, numbers, and operations of ... Federal Air Marshals, to the extent it is not classified national security information;....

See 49 CFR § 1520.5(b)(8) (2004).

<sup>114</sup> Including:

information regarding security screening under aviation or maritime transportation security requirements of Federal law: (i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person; (ii) Information and sources of

(continued...)

respect to the regulation's application to information governed by the language in the MTSA, TSA indicated that "[w]hile the MTSA provides broad limitations on public disclosure of the information related to maritime security requirements (*see* 46 U.S.C. 70103), it does not establish binding requirements for owners and operators of maritime transportation facilities and vessels to safeguard the information from disclosure."<sup>116</sup> TSA concluded that, because the lack of a legal and regulatory framework was prohibiting dissemination to those that needed it, there was an "immediate need to expand the existing regulatory framework governing information related to aviation security to cover information related to security of maritime transportation."<sup>117</sup>

**Judicial Review of SSI Classification.** Since 2001, the implementation and use of the SSI regulations by TSA have created a number of legal controversies that have resulted in both criminal and civil litigation in federal court. Among these are the reported withdrawal of two federal criminal prosecutions involving TSA baggage screeners for fear that proceeding would require the public disclosure of SSI.<sup>118</sup> Based on an electronic search of both published and unpublished federal court opinions, it appears that there have been more than a dozen reported decisions or orders involving the procedural requirements for the use and/or disclosure of SSI. Two of these reported cases have been criminal prosecutions. In one case, the reviewing court determined that despite the liberal discovery permitted to criminal defendants under the Federal Rules of Criminal Procedure, the government was entitled to withhold information from defendants pursuant to the SSI statute.<sup>119</sup> In the other, the government argued that the information being sought by the defendant was designated SSI and, therefore, protected from the defendant's discovery request. The court, however, decided the case on alternative grounds without addressing the SSI statute or the government claims to protection.<sup>120</sup>

---

<sup>114</sup> (...continued)

information used by a passenger or property screening program or system, including an automated screening system; (iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI; ....

*See* 49 CFR § 1520.5(b)(9) (2004).

<sup>115</sup> The "other information" category includes "[a]ny information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section." *See* 49 CFR § 1520.5(b)(16) (2004).

<sup>116</sup> *Id.*

<sup>117</sup> *Id.*

<sup>118</sup> For a more detailed discussion of the controversies that have arisen as a result of SSI implementation, *see* Mitchel A. Sollenberger, CRS Report RS21727 *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*.

<sup>119</sup> *See United States v. Moussaoui*, 2002 WL 1311736 (E.D. Va. 2002) (ordering defense counsel not to disclose any information designated SSI to the defendant in any form).

<sup>120</sup> *See United States v. Louis*, 2005 WL 180885 (S.D.N.Y. 2005) (granting a government (continued...))

With respect to civil actions involving SSI, the courts appear to be using a variety of procedures to address issues raised by or related to information classified by the government as SSI. The most common procedure appears to be the use of *ex parte*, *in camera* reviews of submitted material.<sup>121</sup> For example, in *Gordon v. F.B.I.*, a Freedom of Information Act suit regarding the administration of TSA's "no fly" and other aviation watch lists, the government claimed numerous SSI exemptions and resisted disclosing information to the plaintiffs.<sup>122</sup> The District Court for the Northern District of California ordered that the government "produce copies of all withheld evidence for the Court's review" as well as ordered that the government review all withheld information to ensure that it was exempted in good faith and provide a detailed affidavit explaining why the material was exempt from disclosure.<sup>123</sup> In response to the information and affidavits received, the plaintiffs argued that TSA had not provided enough detail about the withheld information and that they had not sufficiently segregated non-SSI material from that which received the designation.<sup>124</sup> The court disagreed, noting that it "has reviewed *in camera* all of the redacted SSI and has determined that all of it is properly withheld."<sup>125</sup> In addition, the court also stated, with respect to the segregation issue, "the Court has reviewed each of the SSI redactions *in camera* and had determined that each is properly asserted."<sup>126</sup> Similarly, in *Jifry v. FAA*, which involved a challenge to an FAA order revoking the airmen certificates of several alien pilots on the grounds that they posed security risks, the United States Court of Appeals for the District of Columbia Circuit held that, although SSI had been relied upon by the government in deciding to revoke the certificates, there was no due process violation because, among other procedural protections, the pilots were afforded an "*ex parte, in camera* judicial review" of the entire administrative record.<sup>127</sup>

In addition to the use of *ex parte, in camera* review, several courts have examined claimed SSI exemptions using a more traditional analysis under the Freedom of Information Act (FOIA).<sup>128</sup> The statutes authorizing the classification of information as SSI have been held to be an "exemption 3 statute" thereby, authorizing the withholding of information sought under the FOIA. Generally

---

<sup>120</sup> (...continued)

motion to quash subpoenas and document productions issued to DHS employees on alternative grounds).

<sup>121</sup> See, e.g., *Jifry v. FAA*, 370 F.3d 1174 (D.C. Cir. 2004); *Torbet v. United Airlines, Inc.*, 298 F.3d 1087 (9<sup>th</sup> Cir. 2002); *Boles v. Neet*, 402 F.Supp.2d 1237 (D. Col. 2005); *Gordon v. F.B.I.*, 388 F.Supp.2d 1028 (N.D. Ca. 2005).

<sup>122</sup> *Gordon v. F.B.I.*, 388 F.Supp.2d 1028 (N.D. Ca. 2005)

<sup>123</sup> *Id.* at 1033-34.

<sup>124</sup> *Id.* at 1035.

<sup>125</sup> *Id.*

<sup>126</sup> *Id.*

<sup>127</sup> *Jifry v. FAA*, 370 F.3d 1174, 1183 (D.C. Cir. 2004).

<sup>128</sup> See, e.g., *Electronic Privacy Information Center v. D.H.S.*, 384 F.Supp.2d 100 (D.D.C. 2005); *Judicial Watch, Inc. v. D.O.T.*, 2005 WL 1606915 (D.D.C. 2005).

speaking, in responding to FOIA requests, the government is required to submit a “*Vaughn* Index,” which is a document that describes withheld or redacted documents and explains why each withheld record is exempt from disclosure.<sup>129</sup>

Courts that have been faced with *Vaughn* Indexes claiming protections under the SSI statute have reviewed the sufficiency of the government’s explanations and descriptions with mixed results. In *Electronic Privacy Information Center v. D.H.S.*, the District Court for the District of Columbia held that with respect to one document the court “does not have enough information to gauge whether TSA document E falls under exemption 3.”<sup>130</sup> The court noted that the government merely asserted that the documents contained SSI without any additional details.<sup>131</sup> According to the court, while the government is not required to describe the SSI in such detail as to reveal the information, “they must provide a more adequate description in order to justify the application of the exemption to the withheld material.”<sup>132</sup> As a result, the court ordered the government to submit a supplemental *Vaughn* Index with a more detailed description.<sup>133</sup> Conversely, in *Judicial Watch, Inc. v. D.O.T.* the plaintiffs argued that the government’s *Vaughn* Index was too vague to establish that the withheld documents were covered by exemption 3.<sup>134</sup> The court, noting that the government had submitted a revised *Vaughn* Index along with supporting documents, cited a government provided affidavit indicating that TSA determined the information to be SSI because its release “may reveal a systematic vulnerability of the aviation system or a vulnerability of aviation facilities vulnerable to attack.”<sup>135</sup> Based on the information contained in the revised *Vaughn* Index and supporting documents, the court concluded that “DOT has satisfied its burden of establishing that the challenged documents were properly withheld under [FOIA] exemption 3.”<sup>136</sup> Based on these two reported cases, it appears that the government’s ability to withhold information pursuant to SSI depends largely on the adequacy of the explanations that it provides to the court through its *Vaughn* Index and supporting documentation.

Finally, there have been several reported cases that have utilized alternative procedures for dealing with information deemed by the government to be SSI. These procedures have included ordering the parties to provide the court with recommended security procedures before proceeding;<sup>137</sup> ordering TSA to file a redacted motion for

---

<sup>129</sup> See *Vaughn v. Rosen*, 484 F.2d 820, 826-28 (D.C. Cir. 1973).

<sup>130</sup> *Electronic Privacy Information Center v. D.H.S.*, 384 F.Supp.2d 100, 110 (D.D.C. 2005).

<sup>131</sup> *Id.*

<sup>132</sup> *Id.* (citing *Mead Data Cent. Inc. v. U.S. Dep’t of Air Force*, 566 F.2d 242, 261 (D.C. Cir. 1977); *Vaughn*, 484 F.2d at 827).

<sup>133</sup> See *id.*

<sup>134</sup> See *Judicial Watch, Inc. v. D.O.T.*, 2005 WL 1606915, \*10 (D.D.C. 2005).

<sup>135</sup> *Id.* at \*11.

<sup>136</sup> *Id.*

<sup>137</sup> See *Mariani v. United Airlines, Inc.*, 2002 WL 1685382, \* 2 (S.D.N.Y. 2002).

summary judgment with the court under seal;<sup>138</sup> declining to review a TSA final order classifying information as SSI and advising plaintiffs of their ability to appeal to the Court of Appeals;<sup>139</sup> and finally, ordering that TSA attorneys be present at depositions in order to protect SSI from being disclosed during the questioning of witnesses.<sup>140</sup>

---

<sup>138</sup> See *Kalantar v. Lufthansa German Airlines*, 276 F.Supp.2d 5, 14 (D.D.C. 2003).

<sup>139</sup> See *Ahmed v. American Airlines*, 2003 WL 1973168 \*2 (W.D. Tx. 2003).

<sup>140</sup> See *In Re September 11 Litigation*, 2006 WL 846346 \*10 (S.D.N.Y. 2006).